



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/901,814	07/10/2001	Lassi Hippelainen	975.348USW1	7875

32294 7590 09/13/2005

SQUIRE, SANDERS & DEMPSEY L.L.P.  
14TH FLOOR  
8000 TOWERS CRESCENT  
TYSONS CORNER, VA 22182

EXAMINER

GYORFI, THOMAS A

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 09/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/901,814

Applicant(s)

HIPPELAINEN, LASSI

Examiner

Tom Gyorfi

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 28 June 2005.  
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.  
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 2-17, 19-29 and 31-35 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.  
6) ☒ Claim(s) 2-17, 19-29 and 31-35 is/are rejected.  
7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.  
8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.  
10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |



### DETAILED ACTION

1. Claims 2-17, 19-29, and 31-35 remain for examination. The correspondence filed 6/28/05 amended claim 34.

### **Response to Arguments**

2. Applicant's arguments filed 6/28/05 have been fully considered but they are not persuasive.

Applicant argues, *"It is respectfully submitted that the cited combination fails to disclose or suggest all of the features of claim 14. Specifically, Bussey fails to make up for the admitted deficiencies of Dikmen. As discussed above, Bussey merely discloses that the fake place holder packets are transmitted no further than the corresponding output ports. Thus, the fake place holder packets and the packets are transmitted only internally in order to have a properly operating sorting network within the switch. Thus, the fake packets are not transmitted to an interception gateway element, as recited in claim 14."* Examiner disagrees with this contention, noting that fake packet traffic can indeed be transmitted to other network elements (col. 6, lines 60-65).

Applicant further argues, *"Further, it is respectfully submitted that the cited combination of Dikmen and Bussey can not properly be combined to form the basis of a rejection under 35 U.S.C. 103. Specifically, Dikmen and Bussey are non-analogous art and therefore, one skilled in the art would not combine the inventions disclosed in Dikmen and Bussey. Dikmen is directed to the interception of wireless communications. Bussey is merely directed to a packet switch and only addresses the routing of packets via a switch, but not intercepting packets. Further, Bussey merely provides for a simple and fully working switch in which a sorting network operates properly as a full access interconnection network. See Bussey, column 5 lines 63-64. In contrast, Dikmen is directed to interception activity."* [Emphasis Examiner's] The Dikmen reference contains a similar component capable of switching

network traffic (Dikmen, col. 8, lines 20-45), and as such the Bussey reference is applicable.

The remainder of Applicant's arguments are rebutted for reasons similar to those listed above.

***Claim Rejections - 35 USC § 103***

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Claims 2-3, 7-19, 21-28, and 32-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dikmen et al. (U.S. Patent 6,577,865), and further in view of Bussey Jr. (U.S. Patent 4,797,880).

Referring to Claim 14:

Dikmen discloses an interception method for performing a lawful interception in a packet network, comprising the steps of:

a) providing a first network element having an interception function for intercepting data packets (col 4, lines 35-55);

b) controlling said interception function by an interception control means implemented in a second network element (col 4, lines 10-25); and

c) transmitting an intercepted data packet from said first network element via said packet network to an interception gateway element providing an interface to at least one intercepting authority (col 6, lines 10-35).

Dikmen does not explicitly disclose “wherein said first network element generates fake packets to be transmitted with said intercepted data packets and the fake packets are transmitted from said first network element to said interception gateway element.”

Bussey discloses wherein said first network element generates fake packets to be transmitted with said intercepted data packets and the fake packets are transmitted from said first network element to said interception gateway element (Bussey, col. 5, lines 50-65).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to create and transmit fake packets as part of the system disclosed by Dikmen. The motivation for doing so would be to ensure a constant rate of traffic (Bussey, col. 5, lines 60-65), thereby forestalling any timing analysis of packet data.

Referring to Claim 21:

Dikmen discloses an interception system for performing a lawful interception in a packet network, comprising:

a) a first network element having an interception function for intercepting data packets and comprising a transmitting means for transmitting an intercepted data packet to said packet network (col 4, lines 35-55);

b) an interception control means implemented in a second network element and controlling the interception function (col 4, lines 10-25); and

c) an interception gateway element having a receiving means for receiving said intercepted data packet and an interface means for providing an interface to at least one intercepting authority (col 6, lines 10-35).

Dikmen does not explicitly disclose "wherein said first network element further comprises a means for generating fake packets to be transmitted with said intercepted data packets."

Bussey discloses wherein said first network element further comprises a means for generating fake packets to be transmitted with said intercepted data packets (col. 5, lines 50-65).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to create and transmit fake packets as part of the system disclosed by Dikmen. The motivation for doing so would be to ensure a constant rate of traffic (Bussey, col. 5, lines 60-65), thereby forestalling any timing analysis of packet data.

Referring to Claims 2 and 19:

Dikmen and Bussey disclose the limitations of Claims 14 and 21 above. Dikmen further discloses said interception gateway element is integrated in said second network element (Fig. 3; col 5, lines 35-50).

Referring to Claims 3 and 22:

Dikmen and Bussey disclose the limitations of Claims 14 and 21 above. Dikmen further discloses a header of a data packet is read by said second network element and data packets to be intercepted are duplicated (col 4, line 45-col 5, line 15).

Referring to Claims 7 and 28:

Dikmen and Bussey disclose the limitations of Claims 14 and 21 above. Dikmen further discloses said first network element is provided in each network segment of said packet network (col 4, lines 35-65).

Referring to Claim 8:

Dikmen and Bussey disclose the limitations of Claim 14 above. Dikmen further discloses received intercepted data packets are collected in said interception gateway element and supplied to an interface of said at least one intercepting authority (col 5, lines 5-35).

Referring to Claim 9:

Dikmen and Bussey disclose the limitations of Claim 8 above. Dikmen further discloses said interface comprises a first interface for administrative tasks, a second interface for network signaling, and a third interface for intercepted user data (col 1, lines 50-65; col 4, lines 10-45).

Referring to Claim 10:

Dikmen and Bussey disclose the limitations of Claim 14 above. Dikmen further discloses said intercepting function comprises a packet sniffing and filtering function (col 7, lines 20-30).

Referring to Claim 11:

Dikmen and Bussey disclose the limitations of Claim 10 above. Dikmen further discloses said intercepting function is implemented in the Gn interface (col 7, lines 10-35).

Referring to Claim 12:

Dikmen and Bussey disclose the limitations of Claim 14 above. Dikmen further discloses said interception function comprises reading data packets, analyzing the header of the data packets as to whether the data packet should be intercepted or not, and transmitting the data packet to said interception gateway element, and a management function for interception and transmission criteria (col 4, line 40-col 5, line 15).

Referring to Claim 13:

Dikmen and Bussey disclose the limitations of Claim 14 above. Dikmen further discloses an alarm is transmitted to said interception gateway element and all



Art Unit: 2135

interception information of a respective network element is deleted, when a breakage of a casing of the respective network element has been detected (col 3, lines 40-50).

Referring to Claim 15:

Dikmen and Bussey disclose the limitations of Claim 14 above. Bussey further discloses wherein said fake packets are transmitted at random or triggered at any passing packet, such that the total load of intercepted and fake packets transmitted to said interception gateway element is constant (col. 5, lines 60-65).

Referring to Claims 16 and 23:

Dikmen and Bussey disclose the limitations of Claims 14 and 22 above. Dikmen further discloses said intercepted data packet is padded to a maximum length (col 5, lines 1-2).

Referring to Claim 17:

Dikmen and Bussey disclose the limitations of Claim 14 above. Dikmen further discloses a time information is added to said intercepted data packet (col 5, lines 1-2, 55-65).

Referring to Claim 24:

Dikmen and Bussey disclose the limitations of Claim 21 above. Dikmen further discloses said first network element is a gateway element of said packet network (col 4, lines 35-55).

Referring to Claim 25:

Dikmen and Bussey disclose the limitations of Claim 21 above. Dikmen further discloses said first network element is a BG, an SGSN or a GGSN (col 4, lines 35-50).

Referring to Claim 26:

Dikmen and Bussey disclose the limitations of Claim 24 above. Dikmen further discloses wherein an interception information defining a data packet to be intercepted is included in a context information supplied to said first network element and used for routing data packets (col 4, lines 40-col 5, line 15).

Referring to Claim 27:

Dikmen and Bussey disclose the limitations of Claim 26 above. Dikmen further discloses wherein said interception control means comprises a storing means for storing an interception list, and wherein said interception control means is arranged to add said interception information to said context information supplied to said first network element (col 4, lines 25-60).

Referring to Claim 32:

Dikmen and Bussey disclose the limitations of Claim 21 above. Dikmen further discloses said first network element comprises a detecting means for detecting a malfunction and/or breakage thereof, and signaling means for signaling an alarm to said interception gateway element in response to an output of said detecting means (col 3, lines 40-50; col 5, lines 55-65).

Referring to Claim 33:

Dikmen discloses a network element for a packet network, comprising:

- a) an interception means for intercepting a data packet received from said packet network (col 4, lines 10-25), and
- b) a transmitting means for transmitting said intercepted data packet via said packet network to an interception gateway element (col 6, lines 10-35),
- c) wherein said interception means is controlled by an interception control means arranged in another network element (col 4, lines 35-50).

Dikmen does not disclose "said network element further comprises a means for generating fake packets to be transmitted with said intercepted data packets and the fake packets are transmitted from said network element to said interception gateway element."

Bussey discloses said network element further comprises a means for generating fake packets to be transmitted with said intercepted data packets and the fake packets

Art Unit: 2135

are transmitted from said network element to said interception gateway element (col. 5, lines 50-65).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to create and transmit fake packets as part of the system disclosed by Dikmen. The motivation for doing so would be to ensure a constant rate of traffic (Bussey, col. 5, lines 60-65), thereby forestalling any timing analysis of packet data.

5. Claims 4-6, 20, 29, 31, 34, and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dikmen and Bussey as applied to claims 14 and 21 above, and further in view of Aziz et al. (U.S. Pre-Grant Publication 2003/0037235).

Referring to Claim 4:

Dikmen and Bussey disclose the limitations of Claim 14 above.

Neither Dikmen nor Bussey explicitly disclose "intercepted data packet is transmitted to said interception gateway element using a secure tunnel".

Aziz discloses intercepted data packet is transmitted to said interception gateway element using a secure tunnel (paragraphs 0008-0009).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Dikmen in view of Bussey such that the intercepted information is kept secure by using a tunnel. One of ordinary skill in the art would have been motivated to do this because it would provide a method to prevent unauthorized access (Dikmen: col 7, lines 50-60).

Referring to Claim 5:

The combination of Dikmen, Bussey, and Aziz discloses the limitations of Claim 4 above. Aziz further discloses said secure tunnel is implemented by an encryption processing (paragraphs 0008-0009).

Referring to Claim 6:

Dikmen and Bussey disclose the limitations of Claim 14 above.

Neither Dikmen nor Bussey explicitly disclose "said intercepted data packet is transmitted via interworking units and encrypted between said interworking units, when said first network element and said interception gateway element are arranged in separate network segments."

Aziz discloses said intercepted data packet is transmitted via interworking units and encrypted between said interworking units, when said first network element and said interception gateway element are arranged in separate network segments. (Fig. 1; paragraphs 0008-0009, 0021)

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Dikmen in view of Bussey such that the intercepted information is kept secure by using a tunnel. One of ordinary skill in the art would have been motivated to do this because it would provide a method to prevent unauthorized access (Dikmen: col 7, lines 50-60).

Referring to Claim 20:

Dikmen and Bussey disclose the limitations of Claim 21 above.

Neither Dikmen nor Bussey explicitly disclose "said first network element further comprises an encrypting means for encrypting said intercepted data packet"

Aziz discloses said first network element further comprises an encrypting means for encrypting said intercepted data packet (Fig. 1; paragraphs 0008-0009, 0021).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Dikmen in view of Bussey such that the intercepted information is encrypted. One of ordinary skill in the art would have been motivated to do this because it would provide a method to prevent unauthorized access (Dikmen: col 7, lines 50-60).

Referring to Claim 29:

Dikmen and Bussey disclose the limitations of Claim 21 above.

Neither Dikmen nor Bussey explicitly disclose "first network element comprises a control means for controlling interception and encryption processing in accordance with an interception setting instruction received from said interception control means"

Aziz discloses said first network element comprises a control means for controlling interception and encryption processing in accordance with an interception setting instruction received from said interception control means (Fig. 1; paragraphs 0008-0009, 0021).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Dikmen in view of Bussey such that the intercepted information is encrypted. One of ordinary skill in the art would have been motivated to do this because it would provide a method to prevent unauthorized access (Dikmen: col 7, lines 50-60).

Referring to Claim 31:

Dikmen discloses an interception system for performing a lawful interception in a packet network, comprising:

- a) a first network element having an interception function for intercepting data packets and comprising a transmitting means for transmitting an intercepted data packet to said packet network (col 4, lines 35-55);
- b) an interception control means implemented in a second network element and controlling the interception function (col 4, lines 10-25); and
- c) an interception gateway element having a receiving means for receiving said intercepted data packet and an interface means for providing an interface to at least one intercepting authority (col 6, lines 10-35), wherein said interception gateway element comprises a memory means for storing received intercepted data packets before supplying them to said interface means (col. 4, lines 50-60), an extraction means for extracting intercepted data packets [from fake data packets] (col. 2, lines 20-30), and a

means for adding time information to said received intercepted data packets before storing them in memory (col. 5, lines 1-2, and 55-65).

Dikmen does not explicitly disclose the use of fake packets in the system. However, Bussey discloses this limitation (col. 5, lines 50-65). It would have been obvious to one of ordinary skill in the art at the time the invention was made to create and transmit fake packets as part of the system disclosed by Dikmen. The motivation for doing so would be to ensure a constant rate of traffic (Bussey, col. 5, lines 60-65), thereby forestalling any timing analysis of packet data.

Neither Dikmen nor Bussey disclose a decryption means for removing an encryption of the received data packets.

Aziz discloses a decryption means for removing an encryption of the received intercepted data packets (paragraph 0010).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the ability to decrypt encrypted packets into the system disclosed by Dikmen. The motivation to do so would be to permit authorized access to intercepted packets (Dikmen, col. 7, lines 50-60).

Referring to Claim 34:

Dikmen discloses an interception gateway element for an interception system of a packet network, comprising:

a) a receiving means for receiving an intercepted data packet via said packet network from a network element having an interception function (col 4, lines 25-65); and



b) an interface means for providing an interface to an intercepting authority (col. 6, lines 10-35); and

c) a memory means for storing received intercepted data packets before supplying them to said interface means (col 4, lines 50-60), an extraction means for extracting intercepted data packets [from fake data packets] (col. 2, lines 20-30), and means for adding a time information to said received intercepted data packets before storing them in memory (col 5, lines 1-2, 55-65).

Dikmen does not explicitly disclose the use of fake packets in the system. However, Bussey discloses this limitation (col. 5, lines 50-65). It would have been obvious to one of ordinary skill in the art at the time the invention was made to create and transmit fake packets as part of the system disclosed by Dikmen. The motivation for doing so would be to ensure a constant rate of traffic (Bussey, col. 5, lines 60-65), thereby forestalling any timing analysis of packet data.

Neither Dikmen nor Bussey explicitly disclose "a decryption means for removing an encryption of the received intercepted data packets."

Aziz discloses a decryption means for removing an encryption of the received intercepted data packets (paragraph 0010).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the ability to decrypt encrypted packets into the system disclosed by Dikmen. The motivation to do so would be to permit authorized access to intercepted packets (Dikmen, col. 7, lines 50-60).

Referring to Claim 35:

Dikmen and Aziz disclose the limitations of Claim 34 above. Dikmen further discloses an interception control means for controlling said interception function of said network element (col 4, lines 10-45).

### ***Conclusion***

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


Applicant's amendment, particularly on claim 34, necessitated the new ground(s) for rejection based on previously cited prior art. A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tom Gyorfi whose telephone number is (571) 272-3849. The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

TAG  
8/29/05



KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100